REMARKS

In the Office Action dated December 10, 2007, claims 2 and 6 were rejected under 35 U.S.C. §112, second paragraph as being indefinite because the Examiner stated it is not clear how the first and second signatures are generated in the step beginning "storing a..." and then at least one of the first and second signatures is generated in the step beginning "implementing at...". The Examiner is correct that original claim 2 required a separate piece of hardware from the postal security device, but the Examiner's assumption is not correct that the first signature is generated in the postal security device and the second signature is generated in hardware unit. In the embodiment that was intended to be covered by original claim 2, both algorithms of the first and second types are stored in the postal security device, and, depending on whether there is a need to secure a communication for the first purpose or a need to secure a communication for the second purpose, the appropriate one of the cryptographic algorithms is then accessed from the postal security device and is implemented (executed) in the separate hardware unit to secure the communication using the appropriate type of communication algorithm therefore.

In order to clarify this point, original claim 2 has been cancelled and new claim 20 is submitted herewith, consistent with the above explanation. Upon review of claims 2-7, Applicant believes that it is possible that similar incorrect interpretation could occur, and therefore new claims have been added corresponding to each of the original dependent claims that are

consistent with the above explanation, in view of the various different alternatives as to where the algorithms (i.e. the implementation programs therefor) can be stored.

All claims are therefore submitted to be in full compliance with all provisions of Section 112, second paragraph.

Claims 1-7 were rejected under 35 U.S.C. §102(b) as being anticipated by Heiden et al. This rejection of original claim 1 is respectively traversed for the following reasons.

In the Heiden et al reference, the Examiner stated cryptographic algorithms of a first type and a second type are used, to generate first and second digital signatures, respectively. Although it is true that in the Heiden et al reference, two digital signatures are employed, these digital signatures are each generated using the same cryptographic algorithm. As is the case within the cryptographic algorithm, if the input (incoming data) that is run through the algorithm differs, the output of the algorithm naturally will be different as well. It is also the case, as with any cryptographic algorithm, that if the algorithm employs variable settings, the same input (incoming signal) can produce different outputs because the variables have changed. For example, if the algorithm uses a random number generator, it is naturally the case that a different random number will be generated upon each execution of the algorithm.

This fact that is common to all cryptographic algorithms, however, does not mean that simply because the same algorithm produces different outputs

at different times, it can be considered, at one time, to be an algorithm of a first cryptographic type and, at another time, to be considered an algorithm of a second cryptographic type.

In the present specification, "true" cryptographic algorithms of different types are provided as examples at page 7, such as the RSA algorithm, a digital signature algorithm (DSA), and an Elliptic Curve Digital Signature Algorithm (ECDSA). These are truly different "types" of cryptographic algorithms because even if each of these different types of algorithms were provided with the identical input data and the settings (variables) in each algorithm were also identical (to the extent this is possible), different outputs still would result because the cryptographic algorithms are of different types. This is in contrast to the single type of algorithm that is disclosed in Heiden et al reference wherein, under identical conditions (i.e. identical input data and identical settings), the output of the cryptographic algorithm also would be identical.

Applicants believe that the terms "cryptographic algorithm of a first type" and "cryptographic algorithm of a second type" as used in the original language of claim 1 are adequate to convey this concept to a person of ordinary skill in the field of securing communications. Nevertheless, claim 1 has been editorially amended to provide a definition of the first and second cryptographic type that is consistent with the above discussion.

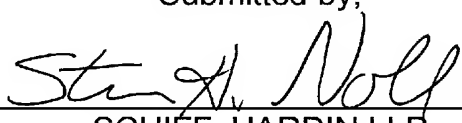
Since the Heiden et al reference does not disclosure or suggest the use of a cryptographic algorithm of a first type and a cryptographic algorithm

of a second type, the Heiden et al reference does not anticipate claim 1, and did not anticipate any of original claims 2-7 depending therefrom. For the same reasons, Applicant submits that the Heiden et al reference does not anticipate any of the new dependent claims that are submitted herein.

Early consideration of the application is respectfully requested.

The Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment to account No. 501519.

Submitted by,



(Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574 Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Applicants.

CH1\5519299.1